

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method for use in a server, comprising:
 receiving at the server a signal representing a request from a remote user for a secure resource residing on a network employing a generic application-layer network protocol;
 determining, without the intervention of the user, the type of security credential for the remote user that is required to access the secure resource; and
 sending from the server a signal representing a second request to the secure resource, the second request including a security credential for the user of the type required to access the secure resource.

Claim 2 (original): The method of claim 1, further comprising:
 authenticating the user before sending the signal representing the second request.

Claim 3 (currently amended): The method of claim 1, further comprising:
 receiving at the server a signal representing a response to the second request; and
 sending from the server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 4 (currently amended): The method of claim 1, wherein the request includes a logon credential for the remote user, the method further comprising:

authenticating the remote user based on the logon credential before sending the second request.

Claim 5 (currently amended): The method of claim 1, wherein the request includes a logon credential for the remote user and the type of security credential required to access the secure resource includes the logon credential, the method further comprising:

 sending the signal representing the second request to the secure resource, the second request including the logon credential.

Claim 6 (currently amended): The method of claim 1, wherein the request includes a logon credential for the remote user, the method further comprising:

 receiving at the server a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential; and
 sending from the server a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes the SSO credential.

Claim 7 (currently amended): The method of claim 6, further comprising:

 sending from the server a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token.

Claim 8 (currently amended): The method of claim 6, further comprising:

 receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

sending from the server a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential.

Claim 9 (original): The method of claim 1, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 10 (currently amended): The method of claim 9; further comprising:
receiving at the server a signal representing data in response to the second request; and
sending from the server a signal representing at least a portion of the data to the remote user.

Claim 11 (currently amended): The method of claim 10, wherein the secure ~~Web~~ resource includes a Web site, and the data is hypertext mark-up language.

Claim 12 (currently amended): The method of claim 1, wherein the receiving includes receiving at the server a signal representing a request from the remote user for a second secure resource residing on the network, the method further comprising:

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

sending from the server a signal representing a third request to the second secure resource, the third request including a security credential for the user of the type required to access the second secure resource; and wherein the signals representing the second and third requests are sent concurrently.

Claim 13 (original): The method of claim 12, wherein the types of security credentials included in the second and third requests differ.

Claim 14 (original): The method of claim 12, wherein the types of security credentials included in the second and third requests are the same.

Claim 15 (currently amended): The method of claim 1, further comprising:
receiving at the server a signal representing the security credential from the user before receiving the signal representing the request.

Claim 16 (currently amended): The method of claim 15, further comprising:
storing the security credential at least until sending the signal representing the second request.

Claim 17 (currently amended): An apparatus for use in a server, comprising:
means for receiving at the server a signal representing a request from a remote user for a secure resource residing on a network employing a generic application-layer network protocol;
means for determining, without the intervention of the user, the type of security credential for the remote user that is required to access the secure resource; and
means for sending from the server a signal representing a second request to the secure resource, the second request including a security credential for the user of the type required to access the secure resource.

Claim 18 (original): The apparatus of claim 17, further comprising:
means for authenticating the user before sending the signal representing the second request.

Claim 19 (currently amended): The apparatus of claim 17, further comprising:
means for receiving at the server a signal representing a response to the second request; and
means for sending from the server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 20 (currently amended): The apparatus of claim 17, wherein the request includes a logon credential for the remote user, the apparatus further comprising:
means for authenticating the remote user based on the logon credential before sending the second request.

Claim 21 (currently amended): The apparatus of claim 17, wherein the request includes a logon credential for the remote user and the type of security credential required to access the secure resource includes the logon credential, the apparatus further comprising:
means for sending from the server the signal representing the second request to the secure resource, the second request including the logon credential.

Claim 22 (currently amended): The apparatus of claim 17, wherein the request includes a logon credential for the remote user, the apparatus further comprising:
means for receiving at the server a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential;
and
means for sending from the server a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes the SSO credential.

Claim 23 (currently amended): The apparatus of claim 22, further comprising:

means for sending from the server a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token.

Claim 24 (currently amended): The apparatus of claim 22, further comprising:

means for receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

means for sending from the server a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential.

Claim 25 (original): The apparatus of claim 17, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 26 (currently amended): The apparatus of claim 25, further comprising:

means for receiving at the server a signal representing data in response to the second request; and

means for sending from the server a signal representing at least a portion of the data to the remote user.

Claim 27 (currently amended): The apparatus of claim 26, wherein the secure Web resource includes a Web site, and the data is hypertext mark-up language.

- Claim 28 (currently amended): The apparatus of claim 17, wherein the means for receiving includes means for receiving at the server a signal representing a

request from the remote user for a second secure resource residing on the network, the apparatus further comprising:

means for determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

means for sending from the server a signal representing a third request to the second secure resource, the third request including a security credential for the user of the type required to access the second secure resource; and

wherein the signals representing the second and third requests are sent concurrently.

Claim 29 (original): The apparatus of claim 28, wherein the types of security credentials included in the second and third requests differ.

Claim 30 (original): The apparatus of claim 28, wherein the types of security credentials included in the second and third requests are the same.

Claim 31 (currently amended): The apparatus of claim 17, further comprising:
means for receiving at the server a signal representing the security credential from the user before receiving the signal representing the request.

Claim 32 (original): The apparatus of claim 31, further comprising:
means for storing the security credential at least until sending the signal representing the second request.

Claim 33 (currently amended): One or more computer-readable ~~Computer-readable~~ media tangibly embodying a program of instructions executable by a computer to perform a method for use in a server, the method comprising:

receiving at the server a signal representing a request from a remote user for a secure resource residing on a network employing a generic application-layer network protocol;

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the secure resource; and

sending from the server a signal representing a second request to the secure resource, the second request including a security credential for the user of the type required to access the secure resource.

Claim 34 (original): The media of claim 33, wherein the method further comprises:

authenticating the user before sending the signal representing the second request.

Claim 35 (currently amended): The media of claim 33, wherein the method further comprises:

receiving at the server a signal representing a response to the second request; and

sending from the server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 36 (original): The media of claim 33, wherein the request includes a logon credential for the remote user, wherein the method further comprises:

authenticating the remote user based on the logon credential before sending the second request.

Claim 37 (currently amended): The media of claim 33, wherein the request includes a logon credential for the remote user and the type of security credential

required to access the secure resource includes the logon credential, wherein the method further comprises:

sending from the server the signal representing the second request to the secure resource, the second request including the logon credential.

Claim 38 (currently amended): The media of claim 33, wherein the request includes a logon credential for the remote user, wherein the method further comprises:

receiving at the server a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential; and
sending from the server a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes the SSO credential.

Claim 39 (currently amended) The media of claim 38, wherein the method further comprises:

sending from the server a signal representing the SSO credential to the secure resource when the type of credential required to access the secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token.

Claim 40 (currently amended): The media of claim 38, wherein the method further comprises:

receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and
sending from the server a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential.

Claim 41 (original): The media of claim 33, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 42 (currently amended): The media of claim 41, wherein the method further comprises:

receiving at the server a signal representing data in response to the second request; and
sending from the server a signal representing at least a portion of the data to the remote user.

Claim 43 (currently amended): The media of claim 42, wherein the Web resource includes a Web site, and the data is hypertext mark-up language.

Claim 44 (currently amended): The media of claim 33, wherein the receiving includes receiving at the server a signal representing a request from the remote user for a second secure resource residing on the network, wherein the method further comprises:

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

sending from the server a signal representing a third request to the second secure resource, the third request including a security credential for the user of the type required to access the second secure resource; and

wherein the signals representing the second and third requests are sent concurrently.

Claim 45 (original): The media of claim 44, wherein the types of security credentials included in the second and third requests differ.

Claim 46 (original): The media of claim 44, wherein the types of security credentials included in the second and third requests are the same.

Claim 47 (currently amended): The media of claim 33, wherein the method further comprises:

receiving at the server a signal representing the security credential from the user before receiving the signal representing the request.

Claim 48 (original): The media of claim 47, wherein the method further comprises:

storing the security credential at least until sending the signal representing the second request.